

RUSSIN, VECCHI
& HEREDIA BONETTI

Protección de Datos en el Teletrabajo y La Realidad Dominicana

3 de marzo 2021

Jose Maldonado Stark

RUSSIN, VECCHI
& HEREDIA BONETTI

- Socio Russin, Vecchi & Heredia Bonetti
- Doctor en derecho de la Universidad Iberoamericana (UNIBE).
- Boston University School of Law, LLM in American Law (Concentration on Corporative Law and Securities Regulation), 2001.
- Maestría en Derecho Fundamentales con la Universidad de Castilla de la Mancha y Pontificia.
- AMCHAMDR Miembro Comité Legal y Energía.
- Miembro E-Commerce y Regulación de la Asociación Dominicana de Empresas Fintech ([ADOFINTECH](#)).
- Miembro pasado del Consejo Directivo Meritas





Protección de Datos en el Teletrabajo y la Realidad Dominicana

- La protección de datos en el teletrabajo es un gran desafío que requiere un compromiso continuo y aunado entre empleadores y trabajadores.
- Ante la implementación e inminente permanencia de esta nueva modalidad, revelaremos las medidas preventivas necesarias para crear una cultura de ciberseguridad.
- Analizaremos los derechos fundamentales que pueden verse comprometidos y los grandes temas litigiosos aplicables a la protección de datos bajo la luz de la Constitución, las leyes y la resolución 23/2020 del Ministerio de Trabajo sobre la regulación del teletrabajo como modalidad especial de trabajo.

Angelina Angelov

RUSSIN, VECCHI
& HEREDIA BONETTI

- Office manager, Russin, Vecchi & Heredia Bonetti.
- Administradora Legal Certificada (CLM).
- Máster en Administración de Empresas (MBA).
- Miembro del Foro Económico Mundial, Inteligencia Estratégica.
- Vicepresidente Comité de Revisión de Productos y Servicios, Association of Legal Administrators ALA (2021-2023).
- Miembro de Comité de Relaciones Internacionales de ALA (2019-2021) y (2013-2016).
- Profesora de Post Grado de Programa de Negocios, UNAPEC.
- Autora: www.thetimeofchange.com

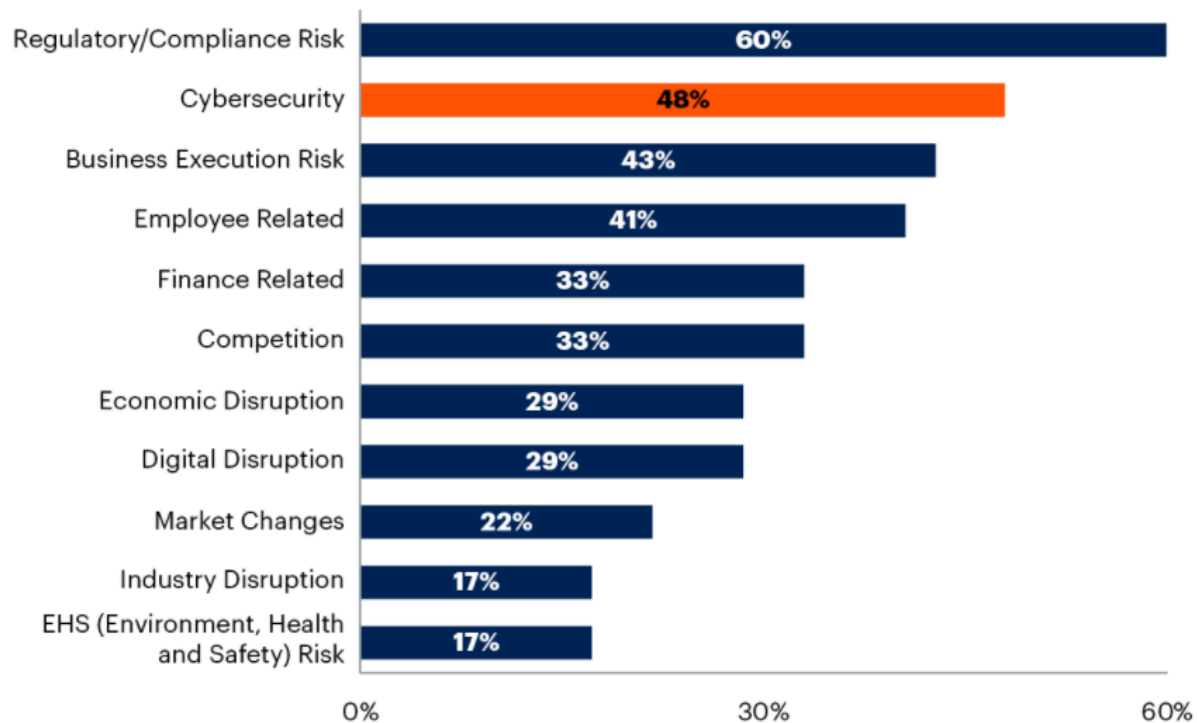


Figure 2: Top Sources of Risk to the Enterprise



Top Sources of Risk to the Enterprise

Percentage of Respondents



n = 133

Q: What are the top sources of risk to the enterprise?

Source: 2020 Gartner Board of Directors Survey

735901_C

Business & Practice

Tuesday, February 2, 2021

Goodwin Procter Says It Was Hit by Data Breach of Vendor

Goodwin Procter fell victim to a data breach after a vendor it uses for large file transfers recently reported it was hacked, according to an internal memo obtained by Bloomberg Law.

The memorandum circulated by Goodwin managing partner Mark Bettencourt on Tuesday said Goodwin was informed of the security issue on Jan.22, and immediately stopped using the service.

The firm also retained a third-party forensic expert and launched an investigation. Goodwin confirmed the veracity of Bettencourt's memo, but declined to comment further.

Cyber breaches have become a growing issue for Big Law firms, which possess an abundance of valuable data and privileged information belonging to attorneys and clients on their networks.

Goodwin's breach investigation revealed that a "small percentage" of the firm's clients "may have experienced unauthorized access to or acquisition of confidential material"

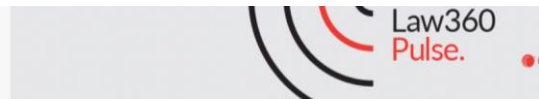
TEN SECTORS WITH MOST FREQUENTLY BREACHED CREDENTIALS

JANUARY 2018 - JUNE 2020

- 31% TECHNOLOGY
- 14% FINANCIAL SERVICES
- 16% FOOD & BEVERAGE
- 6% HEALTHCARE
- 5% RETAIL
- 5% BANKS
- 3% INSURANCE
- 3% EDUCATION
- 3% AUTOMOBILE & PARTS
- 2% TRAVEL & LEISURE



digital shadows_



Don't want ads? [Subscribe](#) or [login now](#)

Jones Day Hit By Third-Party Data Breach

Law360 (February 16, 2021, 5:21 PM EST) -- Hackers may have stolen documents from Jones Day as part of a cyberattack on a third-party vendor that the BigLaw giant uses to transfer files, the firm said Tuesday. An undisclosed amount of information was stolen in the data breach at Palo Alto, California-based cloud computing provider Accellion. (Monika Skolimowska/picture alliance via Getty Images) The law firm, which has 9,600 attorneys worldwide and generated



Ciberseguridad:

Retos

Políticas

Cultura

El año de los gusanos

Infección del primer gusano informático



© 1990 Bettmann/Corbis

Robert Tappan Morris, estudiante de la Cornell University libera lo que más tarde será conocido como el **morris worm** desde el MIT con la intención inicial de estimar el tamaño de Internet. El gusano se extiende masivamente a través de sistemas **Unix** aprovechando varias vulnerabilidades de este sistema operativo. Se estima que el coste ocasionado por el gusano y su eliminación fue de millones de dólares y que infectó a unas 6.000 máquinas solo en la universidad. **Morris** fue condenado en 1990 a tres años de libertad condicional, 400 horas de servicios a la comunidad, una multa de 10.050 dólares y a pagar los costes de su supervisión. **Morris** cofundó en 1995 **Viaweb** y la venderá por 48 millones de dólares a **Yahoo!** en 1998. Desde 2006 es profesor funcionario del MIT y ganador en 2010 del premio **SIGOPS Mark Weiser**.

1988 ve el nacimiento de otro tipo de gusanos de la mano de **IBM**, los dispositivos de almacenamiento **WORM** (Write Once, Read Many). En este año se introducen los protocolos **SMTP** y **NTP** y se funda **ARCHOS**, **Linksys**, **TrendMicro**, **SanDisk** y la **Open Software Foundation (OSF)**.



© 2013 bluestoragemedia

Fueron titulares...
Instalada base española en la Antártida
Un incendio arrosa al centro de Lisboa

1988

Nacimientos

Emma Stone (actriz)
Ai Kago, Rihanna y Adele (cantantes)
Angel Di Maria, Juan Mata, Sergio Agüero, Sergio Busquets y Mesut Özil (futbolistas)
Natascha Kampusch (escritora)



Estrenos TV

Aquellos maravillosos años
Denver, el último dinosaurio
El precio justo
Los cuentos de Alf
Los mundos de Yupi
Roseanne
Rockopop



© 1993 ABC

Cartelera

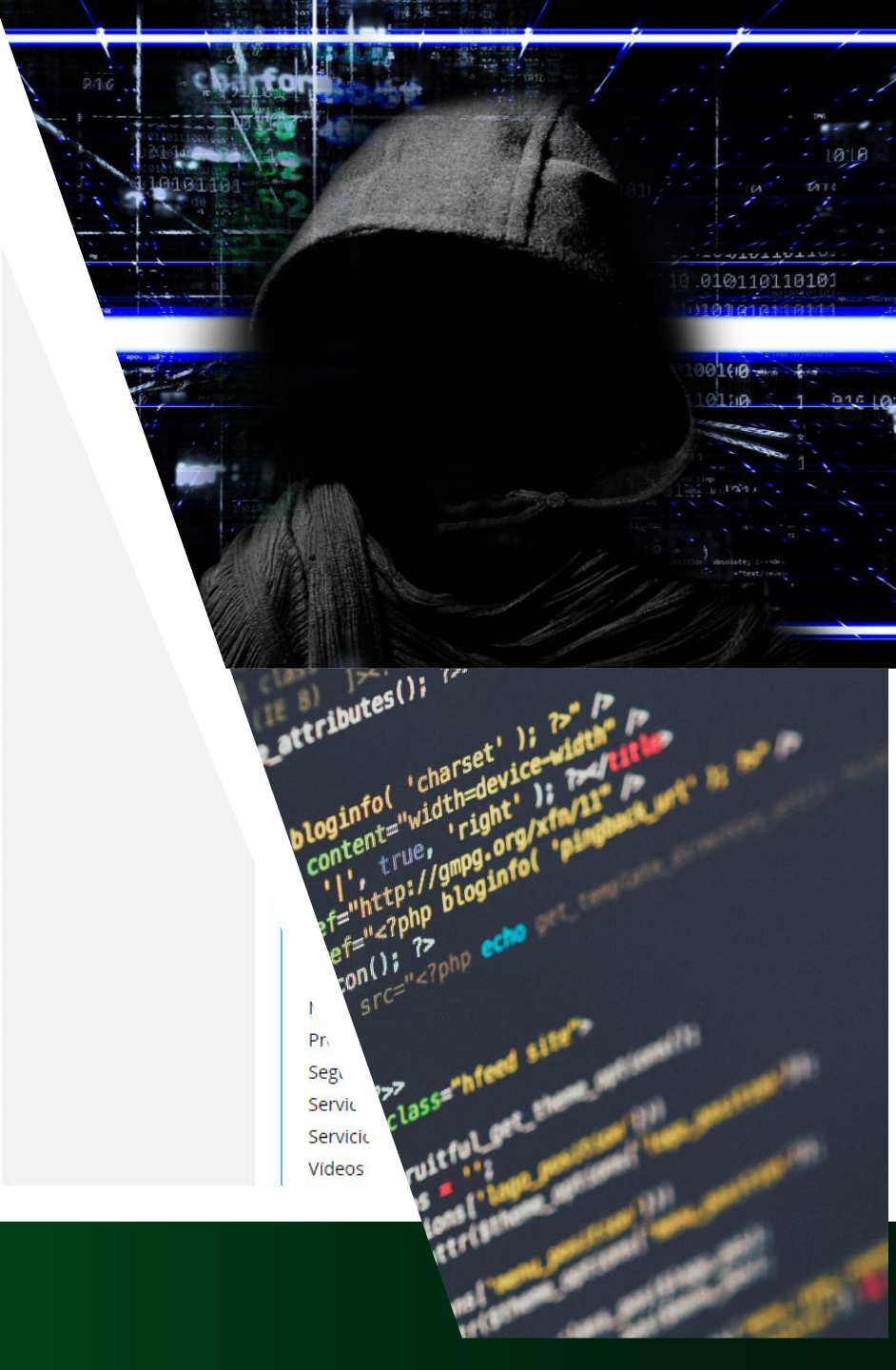
Akira
Bitechus
Cinema Paradiso
Gorilas en la niebla
La Jungla de Cristal
La última tentación de Cristo
Mujeres al borde de un ataque de nervios
Rain man
Un pez llamado Wanda



© 1988 20th Century Fox

En la radio...

A Woman Loves a Man
(Joe Cocker)
(Chaz) Y aparezco a tu lado (Alex y Cristina)





POLÍTICAS DE SEGURIDAD CIBERNÉTICA

La protección incluye:

- Base de datos física y electrónica de los empleados
- Base de datos física y electrónica de los clientes
- Informaciones financieras física y electrónica de los clientes y de su empresa

Los tres ejes de seguridad que abarca son:

- Seguridad física
- Seguridad Técnica y
- Seguridad Administrativa

Estrategia

- Incluir la ciberseguridad en la estrategia de transformación y desarrollo digital de la empresa
- Incluir el tema como parte de agenda de la junta del Consejo Directivo
- Personal técnico debe participar activamente en la planificación estratégica y de continuidad
- Las políticas de seguridad cibernética se basarán en la Evaluación de Riesgo de la firma

Capacitaciones

- Cursos especiales, pruebas y simulaciones
- Construir una cultura de seguridad dentro de las organizaciones
- Aumentar la conciencia sobre la seguridad cibernética
- Mejorar la resistencia del personal al phishing e ingeniería social

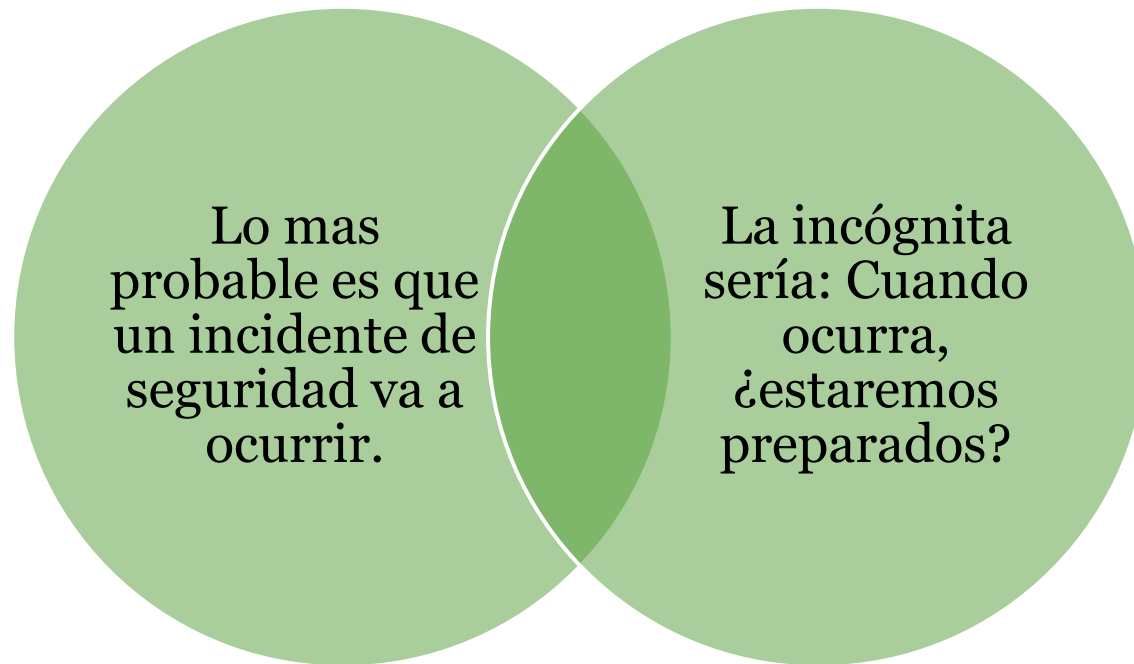
Contrate los expertos

- Necesidades de ciberseguridad necesitan recursos financieros y humanos
- Mayor experiencia
- Cuentan con equipos y personal calificado
- Puede ahorrar dinero, recursos y proteger el negocio

Usar tecnología para reforzar las políticas

- Cambios de contraseñas
- Uso de contraseñas con características específicas
- Desactivar los puertos USB
- No permitir acceso a determinadas páginas
- Bloqueo de sistemas por inactividad

Plan de respuesta



Gestión de Riesgo

- Involucrar Alta Gerencia
- Identificar de la situación actual
- Incluir la ciberseguridad en el perfil de riesgo de la empresa.
- Diseñar acciones de respuesta en caso de incidentes
- Plan de comunicación con los stakeholders

RUSSIN, VECCHI

& HEREDIA BONETTI

- Mitigación de riesgos de manera integral
- Programas de cumplimiento
- Apoyo equipo de respuesta a incidentes
- Comunicación
- Políticas de retención de datos

Parabras Claves

- Asesor Jurídico
- Asesor Jurídico Corporativo
- Responsable de Auditoría Interna
- Legal
- Cumplimiento
- Riesgo
- Privacidad
- Abogado
- Paralegal

RUSSIN, VECCHI
& HEREDIA BONETTI

Cybersecurity is Everyone's Job

National Initiative for Cybersecurity Education



Buenas prácticas

- NO colocar sus contraseñas escritas en un “post it”
- Mantener los archivos personales separados de los de la oficina
- NO dejar que sus hijos menores utilicen los dispositivos donde tienen la data de la oficina
- Usar la encriptación, pero recordar que **deben salvaguardar la clave o la contraseña usada para encriptar. No existen caminos alternativos para abrir datos previamente encriptados**
- Memorias USB: Encriptadas

RUSSIN, VECCHI
& HEREDIA BONETTI

CIBERSEGURIDAD EN EL TELETRABAJO

www.rvhb.com



Maria Waleska Alvarez

Presidente Ejecutiva NAP del Caribe

- Especialista en transformación digital, innovación, tecnologías de información y telecomunicación
- Presidenta ejecutiva de NAP del Caribe
- Licenciada en Derecho por la Pontificia Universidad Católica Madre y Maestra (PUCMM) con mención honorífica Magna Cum Laude
- 1er. Certified Fraud Examiner (CFE) de RD a nivel internacional
- Miembro del Consejo de Directores de EDUCA
- Miembro de la Junta Directiva de ADOFINTECH
- Presidenta del Comité TIC y miembro del consejo de directores de AMCHAMRD
- En el 2019 fue reconocida por el gobierno de Reino Unido en el programa Líderes Internacionales, siendo la primera mujer dominicana figurando junto a 300 líderes de todo el mundo
- Entre 2005-2011 formó parte de la división internacional de Terremark Worlwide desarrollando e implementado los NAPs en América Latina, Caribe y Europa.
- Participó activamente en el proceso de negociación de la Cumbre Mundial sobre la Sociedad de la Información y el Conocimiento de Naciones Unidas y la Unión Internacional de Telecomunicaciones





nap^{del}
caribe

QUIENES SOMOS

- Único Network Access Point de la Región (NAP).
- Seguridad, resiliencia y redundancia.
- Diseñado, construido y operado para ofrecer soluciones de Recuperación de Desastres y Continuidad de Negocios.
- Especializado en soluciones de Data Center, Cloud público y privado y Ciberseguridad.
- En el 2019 expandimos nuestra gestión comercial hacia Centroamérica y Caribe, a través de NAP IT Solutions, división internacional.

2021

¿DONDE NOS ENCONTRAMOS?

El Ecosistema Digital donde vivimos

JAN
2021

DIGITAL AROUND THE WORLD

ESSENTIAL HEADLINES FOR MOBILE, INTERNET, AND SOCIAL MEDIA USE

INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** WITH PREVIOUS REPORTS

TOTAL
POPULATION



7.83
BILLION

URBANISATION:
56.4%

UNIQUE MOBILE
PHONE USERS



5.22
BILLION

vs. POPULATION:
66.6%

INTERNET
USERS*



4.66
BILLION

vs. POPULATION:
59.5%

ACTIVE SOCIAL
MEDIA USERS*



4.20
BILLION

vs. POPULATION:
53.6%



we
are
social



KEPIOS

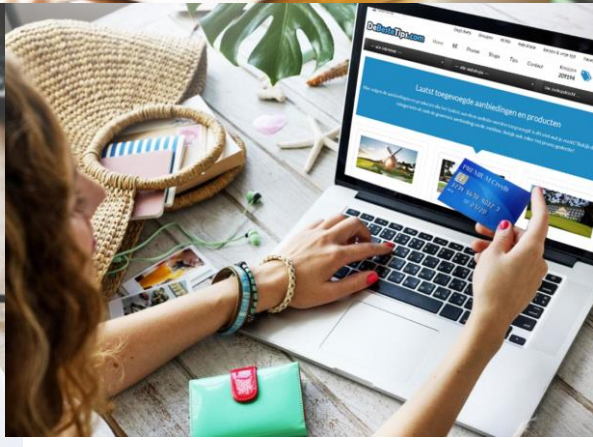
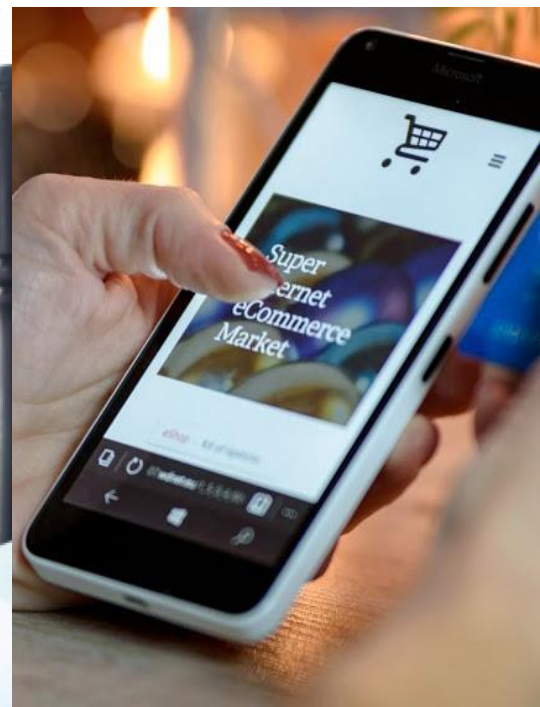
SOURCES: THE U.N.; LOCAL GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; GWI; EUROSTAT; CNNIC; APJII; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; COMPANY EARNINGS REPORTS; MEDIASCOPE. ***ADVISORIES:** INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** TO DATA PUBLISHED IN PREVIOUS REPORTS. SOCIAL MEDIA USER NUMBERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. ♦ **COMPARABILITY ADVISORY:** SOURCE AND BASE CHANGES.

we
are
social

 **Hootsuite***



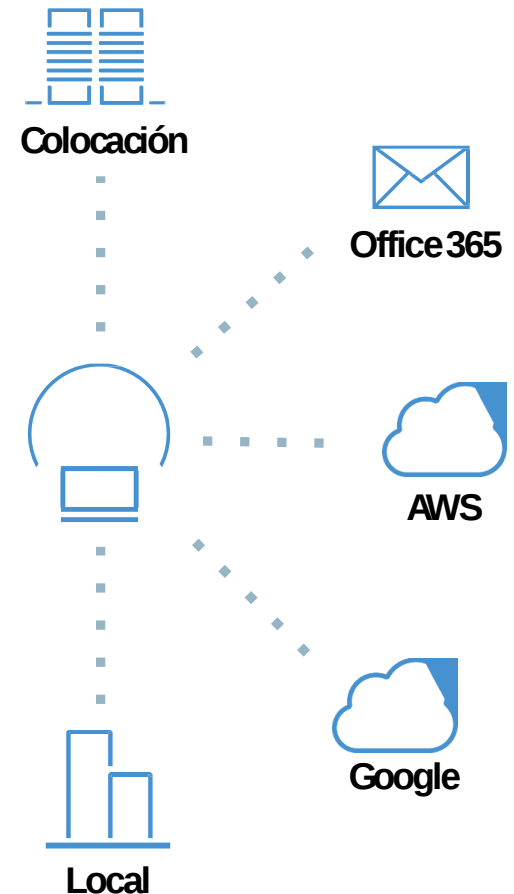
LA EXPECTATIVA DEL CLIENTE



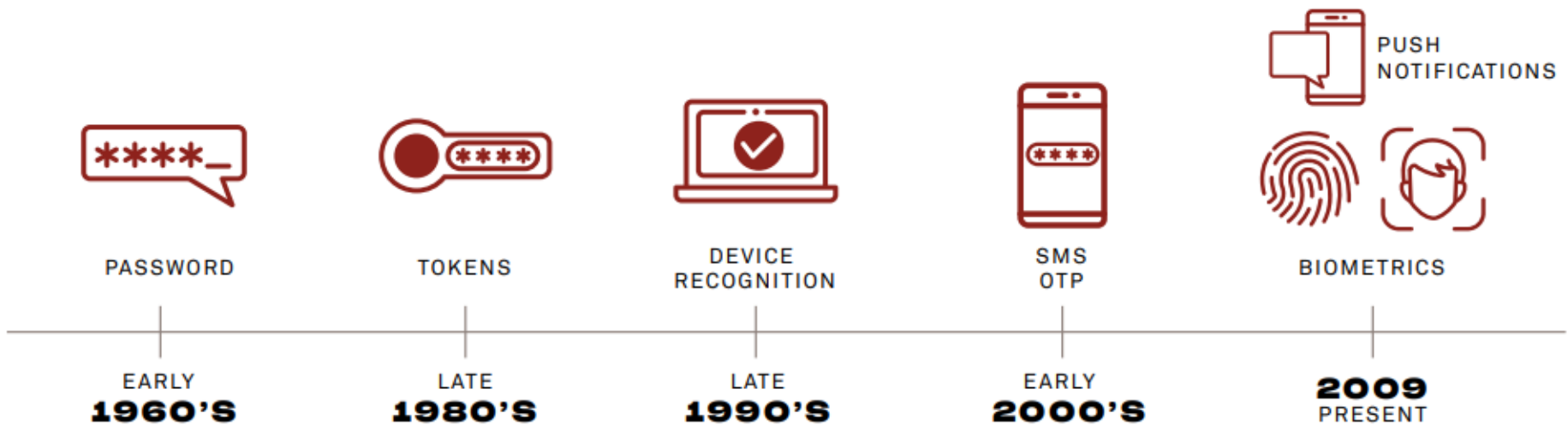
La IT cambió

La SEGURIDAD no

- La IT híbrida eliminó el perímetro
- La ciberseguridad es demasiado lenta o estática
- Muy básica e incapaz de extenderse
- Se construye alrededor de la red, no de los usuarios
- Centralizada, definida por hardware y monolítica



La evolución de la autenticación

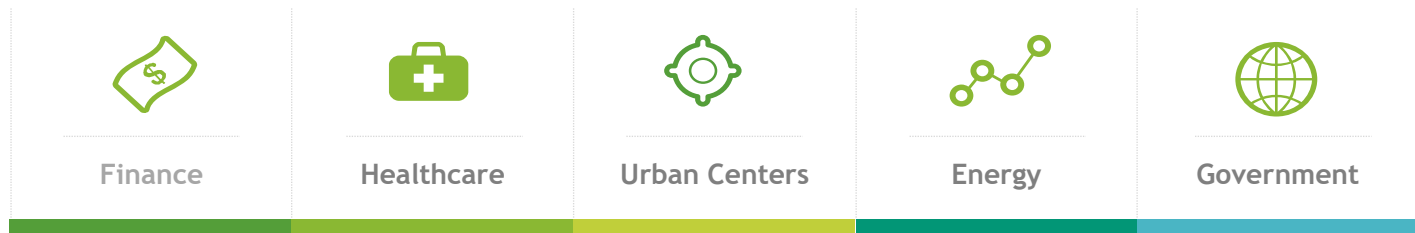


Impacto de los Ecosistemas Digitales

What are the effects? **Adapt or Die**

The average life of a multinational corporate Fortune 500 or its equivalent is 40-50 years

Positive:



Negative:

Cybersecurity threats present the biggest danger since Nuclear War

Critical Infrastructure / Natural Disasters

Protecting and managing the unprecedented amounts of data is critical



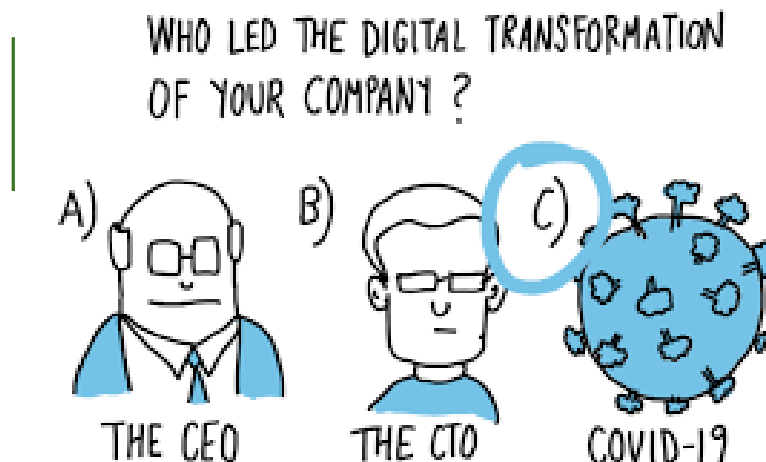
UN REPASO AL 2020



“El año 2020 demostró la capacidad de los delincuentes para invertir tiempo y recursos en ataques más lucrativos, como el ransomware. Además, se están adaptando a la nueva era del trabajo remoto con acciones más sofisticadas para engañar a las víctimas y acceder a las redes corporativas”.

Gartner

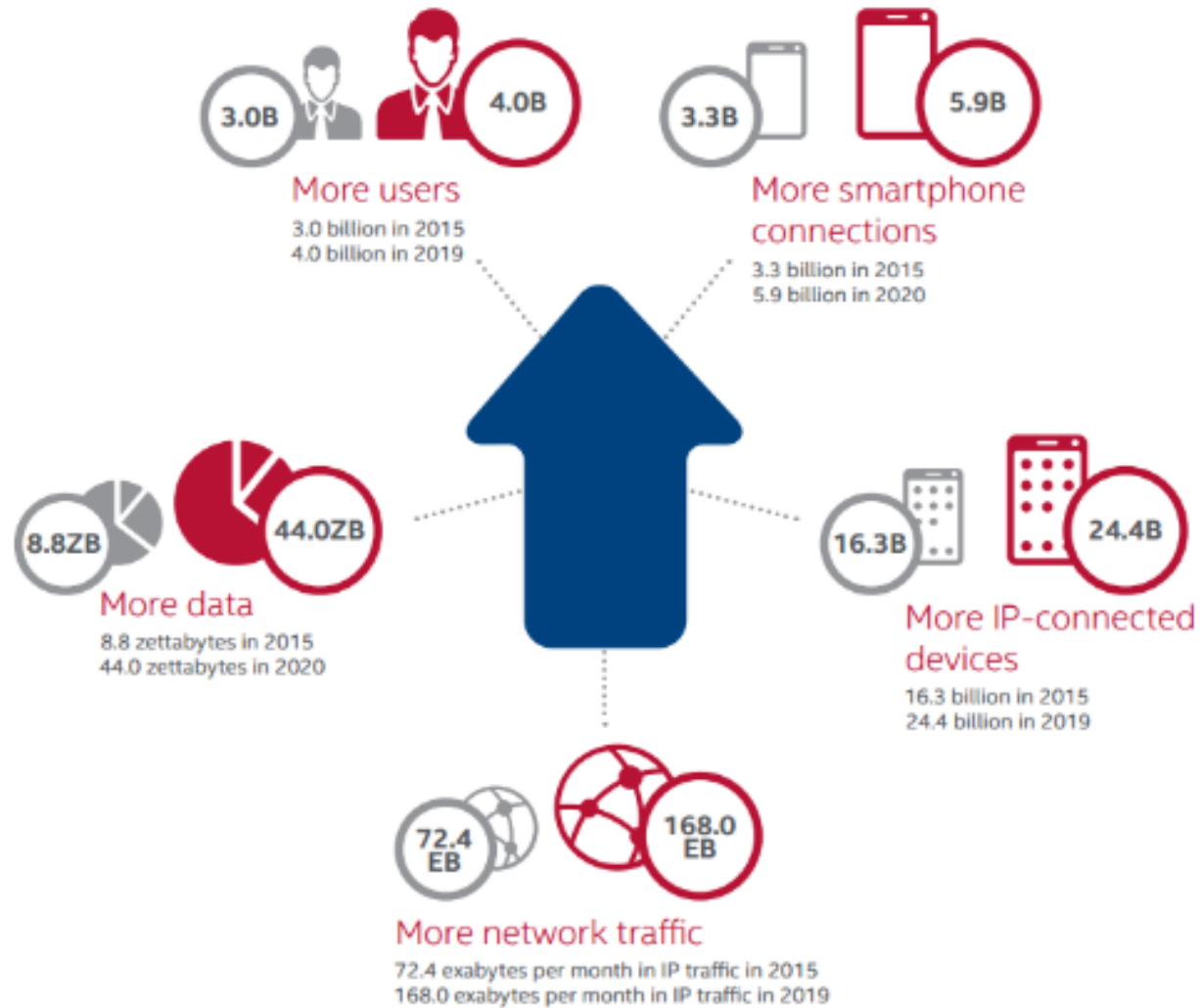
“COVID-19 ha acelerado una tendencia existente en la que la mayoría de los activos y dispositivos se encuentran ahora fuera de los parámetros de seguridad física y lógica”.



Número de notificaciones de brechas de seguridad en 2019. Fuente: AEPD. Elaboración: Bit Life Media



The Growing Cyberattack Surface



Source: McAfee Labs, 2015.

Se produjo un aumento del 345% en usuarios víctimas de engaños a personas haciéndose pasar por una empresa, persona o servicio durante el año pasado.

COVID-19:

La necesidad y la urgencia que tuvieron las empresas para adoptar plataformas digitales como una respuesta a los retos que impuso la pandemia, fue la oportunidad perfecta para que los ciberdelincuentes realizarán ataques focalizados y efectivos.

Aproximadamente,

18 millones

de malware, correos electrónicos de phishing y

**más de 240 millones de mensajes basura
relacionados con el virus,**

son enviados diariamente desde Gmail.

COVID-19:

Uno de los engaños más populares fueron los relacionados con las vacunas, las curas y el tratamientos contra el virus.

Más de 22.000 nuevos dominios que prometían la ventas de equipos de protección, desinfectantes y medicamentos fueron creados en tan sólo un par de semanas.

El año pasado se presentaron aproximadamente 3,950 casos de filtración de datos, casi el 80% sucedió por credenciales robadas o ataques de fuerza bruta

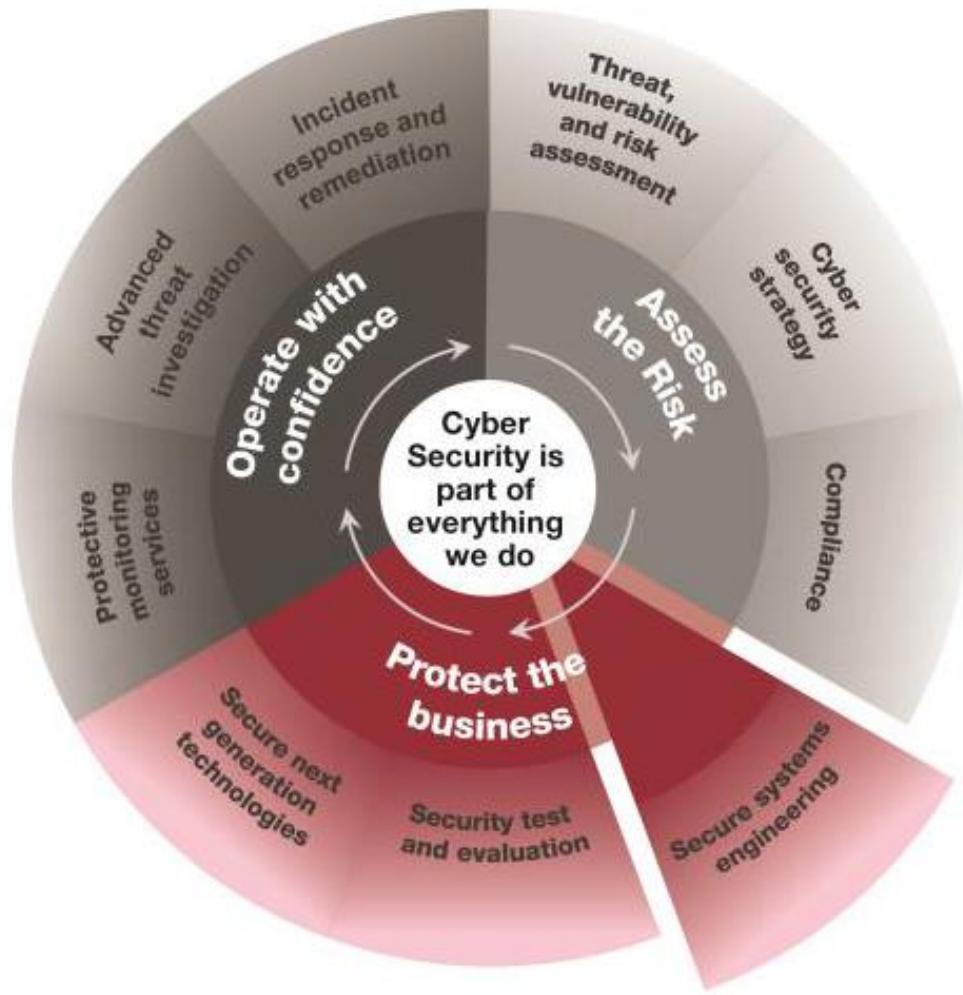
El ciberdelito le cuesta a la economía global 2.9 millones de dólares por minuto, y aproximadamente el 80 por ciento de los ataques están dirigidos al robo de contraseñas

El costo promedio de una filtración de datos en 2020 fue de **\$3.86 millones de dólares**, según informó IBM.



Estas incidencias revelan la importancia para las empresas de tener métodos anti-phishing fuertes.

Estudios reflejan que el **Ransomware y el Password Dumper son los ataques más comunes, donde los cibercriminales lograron encriptar datos en el 73% de los casos reportados.**



CIBERSEGURIDAD COMO ESTRATEGIA

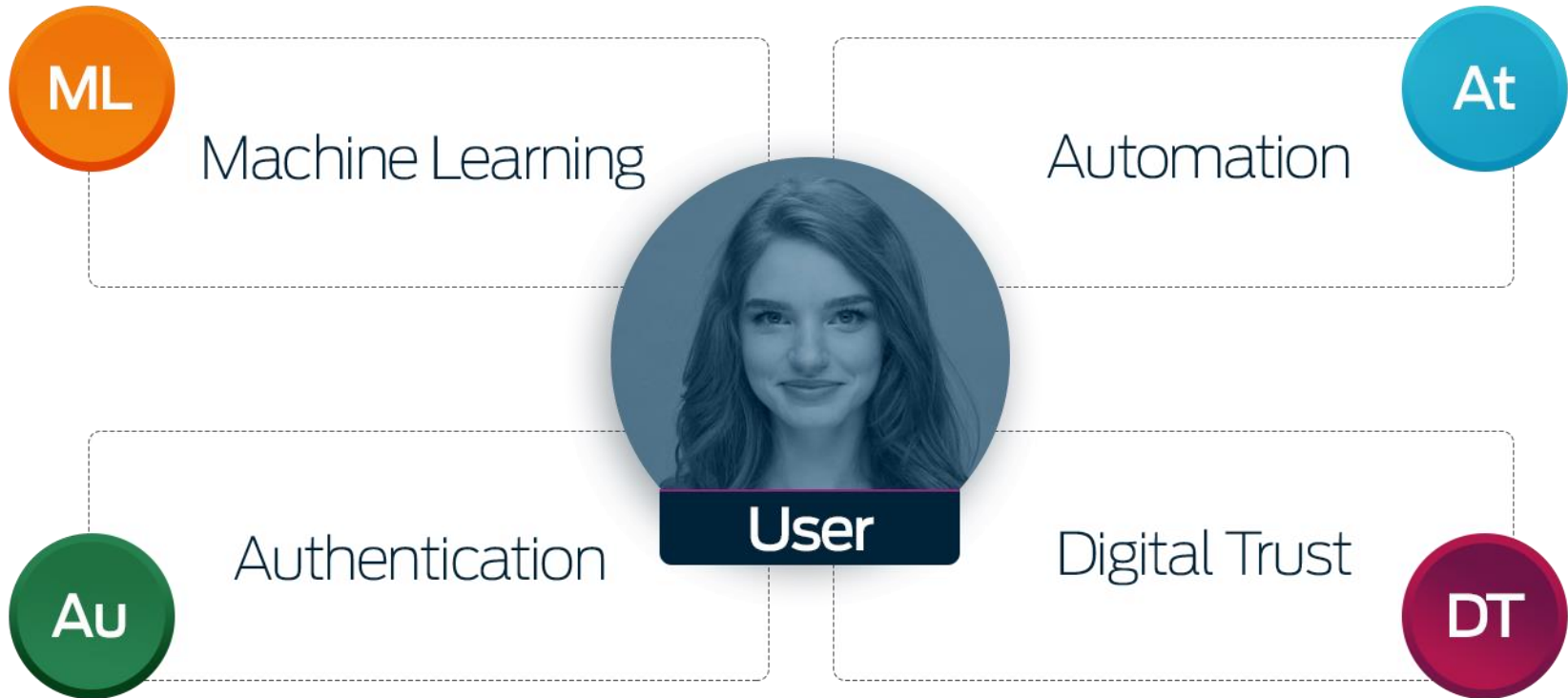
Multi-channel, multi-level approach

Constant comprehensive monitoring

Fast threat deactivation

Never neglect user experience

Future proof





ELEMENTOS ESENCIALES DE UNA ESTRATEGIA DE CIBERSEGURIDAD

REDUCE
LA SUPERFICIE DE ATAQUE

ASEGURA
EL ACCESO

NEUTRALIZA
ADVERSARIOS

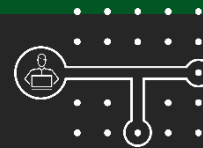
AUTENTICACIÓN MULTIFACTORIAL

Autenticación unificada para toda la población de usuarios de la empresa a través de una completa gama de factores de autenticación.



PERÍMETRO DEFINIDO POR SOFTWARE Y MICROSEGMENTACIÓN

Perímetro de red centrado en la identidad del usuario capaz asegurar cualquier aplicación, en cualquier plataforma y en cualquier lugar.



DIGITAL THREAT PROTECTION

Proactiva identificación y mitigación de amenazas online para minimizar el riesgo digital de las empresas



Jack Welch once said: *"When the external change is faster than the internal change the end is near."*





“Para abordar estos desafíos y hacer frente a los riesgos, los líderes deben valerse de nuevos conocimientos, procesos y herramientas para garantizar el uso responsable de los datos y la resiliencia organizacional”.





nap^{del}caribe



NAP del Caribe

www.napdelcaribe.net.do

Lope de Vega #19, Torre PIISA, Bloque A,
4to piso Suite 401 Naco Santo Domingo
Rep. Dom.

Autopista las Américas, km 27 ½
La Caleta Boca Chica, Parque Cibernético
De Santo Domingo, Rep. Dom.

Joan Manuel Batista Molina

RUSSIN, VECCHI

& HEREDIA BONETTI

- Coordinador Departamento de Litigios Russin, Vecchi & Heredia Bonetti
- Doctor en derecho de la Universidad Iberoamericana (UNIBE).
- Máster en Derecho y Dirección de Empresas en la Universidad de Palermo en Buenos Aires, Argentina.
- Máster en Derecho Administrativo y Gestión Municipal en la Universidad Castilla-La Mancha, España.



RUSSIN, VECCHI
& HEREDIA BONETTI

El Teletrabajo y la protección de datos

Perspectiva dominicana

Charles Darwin

“No es la más fuerte de las especies la que sobrevive, tampoco es la más inteligente la que sobrevive. Es aquella que se adapta mejor al cambio”.



Resolución 23-2020 del 12 de noviembre del 2020 del Ministerio de Trabajo sobre la regulación del teletrabajo como modalidad especial de trabajo.

Protección de datos

- Constitución de la República (Arts. 44 y 70).
- Código Penal de la República Dominicana.
- Ley No. 172-13 sobre Protección de Datos.
- Ley No. 153-98 Ley General de las Telecomunicaciones.
- Ley No. 53-07 Crímenes y Delitos de Alta Tecnología.
- Ley No. 20-00 sobre Propiedad Industrial.
- Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales.
- Resolución No. 055-06 del Instituto Dominicano de las Telecomunicaciones (INDOTEL) que aprueba la norma complementaria de la ley 126-02 sobre Protección de Datos de Carácter Personal por los Sujetos Regulados.

Conceptos y diferencias entre teletrabajo y trabajo a domicilio

Teletrabajo: Modalidad especial de trabajo que se presta a distancia, ya sea de forma parcial o total, **haciendo uso de herramientas vinculadas a las tecnologías de información y comunicación.**

(Artículo segundo de la resolución 23-2020 del Ministerio de Trabajo sobre la regulación del teletrabajo como modalidad especial de trabajo).

Trabajo a domicilio: Es el que ejecutan los trabajadores en el local donde viven, por cuenta de una o más personas físicas o morales, las cuales son consideradas como empleadores.

También es trabajo a domicilio el que es ejecutado por los trabajadores en un local o taller distinto al de las personas por cuya cuenta trabajan

(Art. 266 del Código de Trabajo).-

+

●

○

Artículo séptimo de la Resolución 23-2020 del 12 de noviembre del 2020 del Ministerio de Trabajo sobre la regulación del teletrabajo como modalidad especial de trabajo.

El teletrabajador es responsable de la custodia y uso de la información, tanto de la provista por su empleador para la ejecución del teletrabajo, así como de la generada producto de sus labores, la cual deberá ser usada exclusivamente para la ejecución de sus funciones laborales. Corresponde al empleador informar al teletrabajador sobre la protección y el manejo de datos, así como del riesgo y sanciones que conllevaría el uso indebido de los mismos, y la prohibición del uso de los equipos y/o de las herramientas informáticas por parte de terceros.

Responsabilidades y deberes sobre la información

Artículo séptimo de la
resolución 23-2020.

- **El teletrabajador :**
 - Es responsable de la custodia y uso de la información, tanto:
 - De la información provista por su empleador para la ejecución del teletrabajo, como,
 - De la información generada producto de sus labores.
 - La información deberá ser usada exclusivamente para la ejecución de sus funciones laborales.
- **Corresponde al empleador:**
 - Informar al teletrabajador sobre la protección y el manejo de datos.
 - Informar al teletrabajador del riesgo y sanciones que conllevaría el uso indebido de los mismos.
 - Informar al teletrabajador la prohibición del uso de los equipos y/o de las herramientas informáticas por parte de terceros.

Código de Trabajo (Ley 16-92 Promulgada el 29 de mayo de 1992)

Art. 88.- El empleador puede dar por **terminado** el contrato de trabajo **despidiendo** al trabajador por cualquiera de las causas siguientes:

9. Por revelar el trabajador los secretos de fabricación o dar a conocer asuntos de carácter reservado en perjuicio de la empresa.

Art. 418.- Todo director, dependiente y obrero de fábrica que haya comunicado, o intentado comunicar a extranjeros o dominicanos, residentes en el extranjero, secretos de la fábrica en que está empleado, se castigará con prisión de seis meses, y multa de diez a sesenta pesos.

Se les podrá además privar de los derechos mencionados en el artículo 42, durante uno a tres años, y poner bajo la vigilancia de la alta policía. **Si estos secretos se han comunicado a dominicanos residentes en la República,** la pena será de **uno a tres meses de prisión,** y multa de diez a treinta pesos... *(Sobre las multas ver Ley 12-07)*

Código Penal



Ley 172-13 sobre Protección de Datos

Artículo 5.- Principios. La presente ley se fundamenta en los siguientes principios:

- 5. Seguridad de los datos.
- 6. Deber de secreto.

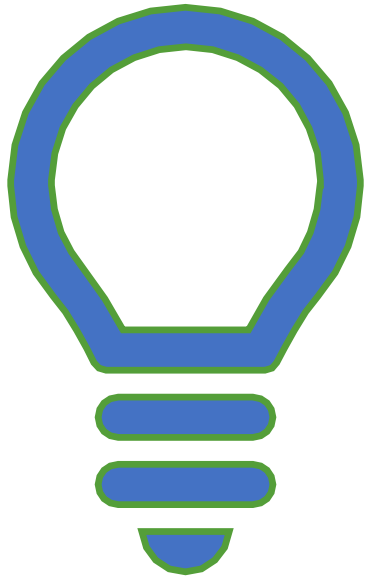
Artículo 88.- Sobre las sanciones: prisión correccional de seis meses a dos años, y una multa de cien (100) a ciento cincuenta (150) salarios mínimos vigentes

Texto modificado mediante sentencia TC/0484/16 de fecha 18 de octubre del 2016

Ley sobre crímenes y delitos de Alta Tecnología. Ley 53-07 de fecha 23 de abril del 2007.

Artículo 10.- Daño o Alteración de Datos. El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas veces el salario mínimo.

Párrafo.- Cuando este hecho sea realizado por un **empleado, ex-empleado o una persona que preste servicios** directa o indirectamente a la persona física o jurídica afectada, las penas se elevarán desde **uno a tres años de prisión y multa** desde **seis hasta quinientas veces el salario mínimo**.



Recomendaciones



Calle El Recodo #2, Edificio Monte Mirador, Tercer piso, Bella Vista,
Santo Domingo, República Dominicana

Tel. (809) 535-9511 • Fax: (809) 535-6649 • info@rvhb.com

Web: www.rvhb.com

Las opiniones emitidas en este Seminario son a Título personal y no necesariamente reflejan las de las organizaciones o firmas de abogados aquí representadas